L Number	Hits	Search Text	DB	Time stamp
1	2787	713/174.ccls. or 713/185.ccls. or 713/192.ccls. or 713/194.ccls. or 713/200-201.ccls. or 713/155.ccls. or 713/168.ccls.	USPAT	2003/12/19 14:56
2	660	705/60.ccls. or 705/62.ccls. or 705/63.ccls. or 705/401.ccls. or 705/408.ccls. or 705/405.ccls. or 705/60.ccls. or 705/410.ccls. or 705/404.ccls.	USPAT	2003/12/19 14:57
3	549	380/51.ccls. or 380/54.ccls.	USPAT	2003/12/19 14:58
4	3882	(713/174.ccls. or 713/185.ccls. or 713/192.ccls. or 713/194.ccls. or 713/200-201.ccls. or 713/155.ccls. or 713/168.ccls.) or (705/60.ccls. or 705/62.ccls. or 705/63.ccls. or 705/401.ccls. or 705/408.ccls. or 705/405.ccls. or 705/60.ccls. or 705/410.ccls. or 705/404.ccls.) or (380/51.ccls. or 380/54.ccls.)	USPAT	2003/12/19 14:58
5	1745	postage near2 meter$4 or frank$4 near2 meter$4	USPAT	2003/12/19 15:04
6	117061	seed$3 or random near2 number	USPAT	2003/12/19 15:04
7	171	(postage near2 meter$4 or frank$4 near2 meter$4) and (seed$3 or random near2 number)	USPAT	2003/12/19 14:59
8	514709	duration or time near2 record or time near2 keep$4 or meter$4	USPAT	2003/12/19 15:00
9	14869	self near2 test3 or test$3 near2 mode	USPAT	2003/12/19 15:05
10	5	((postage near2 meter$4 or frank$4 near2 meter$4) and (seed$3 or random near2 number)) and (self near2 test3 or test$3 near2 mode)	USPAT	2003/12/19 15:02
11	2907	postage near2 meter$4 or frank$4 near2 meter$4	USPAT; EPO; JPO; DERWENT	2003/12/19 15:04
12	208246	seed$3 or random near2 number	USPAT; EPO; JPO; DERWENT	2003/12/19 15:05
13	23566	self near2 test3 or test$3 near2 mode	USPAT; EPO; JPO; DERWENT	2003/12/19 15:05
14	5	(postage near2 meter$4 or frank$4 near2 meter$4) and (seed$3 or random near2 number) and (self near2 test3 or test$3 near2 mode)	USPAT; EPO; JPO; DERWENT	2003/12/19 15:05

L Number	Hits	Search Text	DB	Time stamp
1	2787	713/174.ccls. or 713/185.ccls. or 713/192.ccls. or 713/194.ccls. or 713/200-201.ccls. or 713/155.ccls. or 713/168.ccls.	USPAT	2003/12/19 14:56
2	660	705/60.ccls. or 705/62.ccls. or 705/63.ccls. or 705/401.ccls. or 705/408.ccls. or 705/405.ccls. or 705/60.ccls. or 705/410.ccls. or 705/404.ccls.	USPAT	2003/12/19 14:57
3	549	380/51.ccls. or 380/54.ccls.	USPAT	2003/12/19 14:58
4	3882	(713/174.ccls. or 713/185.ccls. or 713/192.ccls. or 713/194.ccls. or 713/200-201.ccls. or 713/155.ccls. or 713/168.ccls.) or (705/60.ccls. or 705/62.ccls. or 705/63.ccls. or 705/401.ccls. or 705/408.ccls. or 705/405.ccls. or 705/60.ccls. or 705/410.ccls. or 705/404.ccls.) or (380/51.ccls. or 380/54.ccls.)	USPAT	2003/12/19 14:58
5	1745	postage near2 meter$4 or frank$4 near2 meter$4	USPAT	2003/12/19 15:04
6	117061	seed$3 or random near2 number	USPAT	2003/12/19 15:04
7	171	(postage near2 meter$4 or frank$4 near2 meter$4) and (seed$3 or random near2 number)	USPAT	2003/12/19 14:59
8	514709	duration or time near2 record or time near2 keep$4 or meter$4	USPAT	2003/12/19 15:00
9	14869	self near2 test3 or test$3 near2 mode	USPAT	2003/12/19 15:05
10	5	((postage near2 meter$4 or frank$4 near2 meter$4) and (seed$3 or random near2 number)) and (self near2 test3 or test$3 near2 mode)	USPAT	2003/12/19 15:02
11	2907	postage near2 meter$4 or frank$4 near2 meter$4	USPAT; EPO; JPO; DERWENT	2003/12/19 15:04
12	208246	seed$3 or random near2 number	USPAT; EPO; JPO; DERWENT	2003/12/19 15:05
13	23566	self near2 test3 or test$3 near2 mode	USPAT; EPO; JPO; DERWENT	2003/12/19 15:05
14	5	(postage near2 meter$4 or frank$4 near2 meter$4) and (seed$3 or random near2 number) and (self near2 test3 or test$3 near2 mode)	USPAT; EPO; JPO; DERWENT	2003/12/19 15:07
15	892	380/46.ccls. or 380/44.ccls.	USPAT; EPO; JPO; DERWENT	2003/12/19 15:08
16	7	(380/46.ccls. or 380/44.ccls.) and (postage near2 meter$4 or frank$4 near2 meter$4)	USPAT; EPO; JPO; DERWENT	2003/12/19 15:08

```
### Status: Path 1 of [Dialog Information Services via Modem]

### Status: Initializing TCP/IP using (UseTelnetProto 1 ServiceID dialog.com)
Trying 31060000009999...Open

DIALOG INFORMATION SERVICES
PLEASE LOGON:
 ******** HHHHHHHH SSSSSSSS?
### Status: Signing onto Dialog
 ********
ENTER PASSWORD:
 ******** HHHHHHHH SSSSSSSS? ********
Welcome to DIALOG
### Status: Connected


Dialog level 03.05.00D

Last logoff:  19dec03 11:46:23
Logon file405 19dec03 15:12:52
* * *                                * * *
SYSTEM:HOME
Cost is in DialUnits
Menu System II: D2 version 1.7.9 term=ASCII
                     *** DIALOG HOMEBASE(SM) Main Menu ***

 Information:
  1.  Announcements (new files, reloads, etc.)
  2.  Database, Rates, & Command Descriptions
  3.  Help in Choosing Databases for Your Topic
  4.  Customer Services (telephone assistance, training, seminars, etc.)
  5.  Product Descriptions

 Connections:
  6.  DIALOG(R) Document Delivery
  7.  Data Star(R)

    (c) 2003 Dialog, a Thomson business.      All rights reserved.

      /H = Help            /L = Logoff          /NOMENU = Command Mode


Enter an option number to view information or to connect to an online
 service.  Enter a BEGIN command plus a file number to search a database
(e.g., B1 for ERIC).
?b 2,6,8,34,434,35,62,65,77,99,144,94,233,238,266,15,16,239,275,621,636,647,674,9,15,14
8,624,553,267,696

>>>          77 does not exist
>>>         238 does not exist
>>>2 of the specified files are not available
       19dec03 15:14:17 User264815 Session D38.1
            $0.00    0.150 DialUnits FileHomeBase
     $0.00  Estimated cost FileHomeBase
     $0.46  TELNET
     $0.46  Estimated cost this search
     $0.46  Estimated total session cost   0.150 DialUnits


SYSTEM:OS  - DIALOG OneSearch
  File   2:INSPEC  1969-2003/Dec W1
       (c) 2003 Institution of Electrical Engineers
*File   2: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File   6:NTIS  1964-2003/Dec W3
       (c) 2003 NTIS, Intl Cpyrght All Rights Res
  File   8:Ei Compendex(R)  1970-2003/Dec W1
         (c) 2003 Elsevier Eng.  Info. Inc.
  File  34:SciSearch(R) Cited Ref Sci  1990-2003/Dec W2
         (c) 2003 Inst for Sci Info
  File 434:SciSearch(R) Cited Ref Sci  1974-1989/Dec
         (c) 1998 Inst for Sci Info
  File  35:Dissertation Abs Online  1861-2003/Nov
         (c) 2003 ProQuest Info&Learning
  File  62:SPIN(R)  1975-2003/Nov W1
         (c) 2003 American Institute of Physics
  File  65:Inside Conferences  1993-2003/Dec W2
         (c) 2003 BLDSC all rts. reserv.
  File  99:Wilson Appl. Sci & Tech Abs  1983-2003/Nov
         (c) 2003 The HW Wilson Co.
  File 144:Pascal  1973-2003/Dec W1
         (c) 2003 INIST/CNRS
  File  94:JICST-EPlus  1985-2003/Dec W2
         (c)2003 Japan Science and Tech Corp(JST)
  File 233:Internet & Personal Comp. Abs.  1981-2003/Jul
         (c) 2003, EBSCO Pub.
  File 266:FEDRIP  2003/Oct
         Comp & dist by NTIS, Intl Copyright All Rights Res
  File  15:ABI/Inform(R)  1971-2003/Dec 19
         (c) 2003 ProQuest Info&Learning
*File  15: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
  File  16:Gale Group PROMT(R)  1990-2003/Dec 19
         (c) 2003 The Gale Group
*File  16: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
  File 239:Mathsci  1940-2003/Jan
         (c) 2003 American Mathematical Society
  File 275:Gale Group Computer DB(TM)  1983-2003/Dec 19
         (c) 2003 The Gale Group
  File 621:Gale Group New Prod.Annou.(R)  1985-2003/Dec 18
         (c) 2003 The Gale Group
  File 636:Gale Group Newsletter DB(TM)  1987-2003/Dec 19
         (c) 2003 The Gale Group
  File 647:CMP  Computer Fulltext  1988-2003/Dec W2
         (c) 2003 CMP Media, LLC
  File 674:Computer News Fulltext  1989-2003/Dec W1
         (c) 2003 IDG Communications
  File   9:Business & Industry(R)  Jul/1994-2003/Dec 18
         (c) 2003 Resp. DB Svcs.
  File 148:Gale Group Trade & Industry DB  1976-2003/Dec 18
         (c)2003 The Gale Group
*File 148: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
  File 624:McGraw-Hill Publications  1985-2003/Dec 18
         (c) 2003 McGraw-Hill Co. Inc
*File 624: Homeland Security & Defense and 9 Platt energy journals added
Please see HELP NEWS624 for more
  File 553:Wilson Bus. Abs. FullText  1982-2003/Nov
         (c) 2003 The HW Wilson Co
  File 267:Finance & Banking Newsletters  2003/Dec 15
         (c) 2003 The Dialog Corp.
  File 696:DIALOG Telecom. Newsletters  1995-2003/Dec 18
         (c) 2003 The Dialog Corp.

      Set  Items  Description
      ---  -----  -----------
?s postage? (1n) meter? or frank? (1n) machine
           50613  POSTAGE?
          498581  METER?
            2609  POSTAGE?(1N)METER?
         1003207  FRANK?
         1836360  MACHINE
```

```
             343  FRANK?(1N)MACHINE
      S1    2942  POSTAGE? (1N) METER? OR FRANK? (1N) MACHINE
?s random (2n) number? or seed
Processing
Processed  10 of  27 files ...
Completed processing all files
         1047038  RANDOM
         9901006  NUMBER?
           29286  RANDOM(2N)NUMBER?
          312384  SEED
      S2  341119  RANDOM (2N) NUMBER? OR SEED
?s cryptograph? (2n) key?
Processing
Processed  20 of  27 files ...
Completed processing all files
           82970  CRYPTOGRAPH?
         4772470  KEY?
      S3   18787  CRYPTOGRAPH? (2N) KEY?
?s meter? or time? or timing or duration or log?
Processing
Processing
Processed  10 of  27 files ...
Processing
Processing
Processed  20 of  27 files ...
Processing
Processing
Completed processing all files
          498581  METER?
        17174399  TIME?
          657668  TIMING
          629601  DURATION
         3348518  LOG?
      S419951811  METER? OR TIME? OR TIMING OR DURATION OR LOG?
?s self (2n) test? or self (2n) mode or test?
Processing
Processing
Processed  10 of  27 files ...
Processing
Processing
Processed  20 of  27 files ...
Completed processing all files
         2274427  SELF
         9022594  TEST?
           37969  SELF(2N)TEST?
         2274427  SELF
         1733702  MODE
            7509  SELF(2N)MODE
         9022594  TEST?
      S5 9029081  SELF (2N) TEST? OR SELF (2N) MODE OR TEST?
?e au=schwartz,robert

Ref    Items  Index-term
E1         0 *AU=SCHWARTZ,ROBERT
E2         1  AU=SCHWARTZA, J.
E3         1  AU=SCHWARTZACHER, W.
E4        53  AU=SCHWARTZALBIEZ R
E5         3  AU=SCHWARTZAND, EPHRAIM
E6         3  AU=SCHWARTZAPFEL B
E7         2  AU=SCHWARTZAPFEL BETH
E8         1  AU=SCHWARTZAPFEL BL
E9         1  AU=SCHWARTZAPFEL J A
E10        1  AU=SCHWARTZAPFEL, HAROLD B.
E11        1  AU=SCHWARTZAPFEL, JON ADAM
E12        2  AU=SCHWARTZAPFEL, W.

          Enter P or PAGE for more
```

```
?s s3 and s1
           18787  S3
            2942  S1
      S6      38  S3 AND S1
?s s2 and s3
          341119  S2
           18787  S3
      S7     661  S2 AND S3
?s s4 and s2
Processing
Processed  10 of  27 files ...
Processing
Processed  20 of  27 files ...
Processing
Completed processing all files
        19951811  S4
          341119  S2
      S8  102910  S4 AND S2
?s s8 and s1
          102910  S8
            2942  S1
      S9      26  S8 AND S1
```

Google

Advanced Search Preferences Language Tools Search Tips

postage meter and random numb Google Search

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web · Images · Groups · Directory · News ·

Searched the web for **postage meter and random number**. Results **1** - **10** of about **54,400**. Search took **0.29** se

Postage Meter - Compare Prices on **Postage** Equipment & Save! Sponsored Link
www.BuyerZone.com **Postage** Equipment for Less - Compare & Save Now.

Print **Postage** on Your PC Sponsored Link
www.stamps.com Save up to 80% on USPS approved **postage**. Free Digital Scale! Aff.

<html> <head> </head><body><pre>&lt;html&gt; &lt;head&gt; &lt ...
... either a computer-based or **postage meter**-based host ... register) and the total **postage**
value used by ... that may contain an internal **random number** generator, various ...
www.ribbs.usps.gov/files/fedreg/usps96/96-15778.TXT - 9k - Cached - Similar pages

[PDF] Security Policy **Postal** Revenector Version 1.4
File Format: PDF/Adobe Acrobat - View as HTML
... The Customer is the end user of the **postal meter** that shall ... The value is changed by
every **random** generation of the **Postal** ... U D,U,ZU,Z M x **Postage** Value Download ...
csrc.nist.gov/cryptval/140-1/140sp/140sp348.pdf - Similar pages

Postage Meter Regulations
... of the **postage**, the assigned serial **number** and, in ... access to the mechanism of the
postage meter can be obtained only through the use of **random** numerical or ...
laws.justice.gc.ca/en/c-10/sor-83-748/text.html - 29k - Cached - Similar pages

Sweepstakes Frequently Asked Questions from ragstoriches ...
... Is there usually a certain **number** of days that a potential ... By definition a sweepstakes
is a **random** drawing. ... Can I use a **postage meter** on my sweepstakes entries ...
www.ragstoriches.com/FAQ.htm - 15k - Cached - Similar pages

Microsoft Excel Tips Page 21
... Select the cell(s) containing the **random number**(s) you want ... ALL as text--because Excel
can sort "text" **numbers**. ... we have no tips for rigging your **postage meter**. ...
www.tipsdr.com/Microsoft-Excel-Tips-21.html - 39k - Cached - Similar pages

Removable Media (Internal) - 7-14GB 8 mm Tape Drive
... LEDs, **POST** PART 1, **POST** PART 2, **POST** FAILED, READY NO TAPE, ... Fast LED = 4 flashes per
second (3.76Hz) **Random** LED = flash ... The 112 **Meter** Tape part **number** is

Sponsored Links

Pitney Bowes **Postage**
60 Days Free and $30 Free Postage
Pitney Personal Postage Machine.
www.pitneybowes.com
Interest:

Hasler® Digital Meters
Upgrade your old meter to a new
USPS approved digital postage meter
www.haslerinc.com
Interest:

Postage Meter
Huge Selection - Up to 69% Off List
Prices at Viking Office! Shop Here
www.vikingop.com
Interest:

Mail Machine Supplies
Supplies for Pitney Bowes, Neopost,
Ascom Hasler, and Postalia machines
www.mailmachinesupplies.com
Interest:

US Postal Rate Wall Chart
24" x 19" Wallchart with current US
Postal rates, measurements, weights
www.OfficeTimeSavers.com
Interest:

Pitney Bowes
Postage Meter/Scale Start-Up Kit
You can mail anything, any size.
www.officedepot.com
Interest:

Postage Meter
Find the best deal! Compare prices,
Reviews and More - CNET Shopper.com
shopper.cnet.com
Interest:

370-1298-01 ...
sunsolve.sun.com/handbook_pub/Devices/
Removable_Media/RMVBL_7_14GB_8mm.html - 29k - Cached - Similar pages

Introduction
... where P is the specific **post**-spacing in **meters**, X a is ... 2, n can be determined at varying
nominal **post**-spacing in ... on x and/or y axis rather than **random** selection ...
www.cla.sc.edu/geog/rslab/751/Projects_2001/ Chowte/final_project.htm - 83k - Cached - Similar pages

Postage Meters
... when required for use in **random** surveys to ... All components except the **postage meter** may be purchased ... specifications, can automatically feed, **meter**, seal, and ...
www.tpub.com/content/administration/ 14198/css/14198_35.htm - 26k - Cached - Similar pages

AAR: Publication: eCommerce patent bulletin: Australia - accepted ...
... a hashing operation, wherein the table of **random numbers** is generated ... the remote client computer functions as a **meter** client on the **postage** metering network ...
www.aar.com.au/pubs/patent/71/ausacc.htm - 70k - Cached - Similar pages

Monitoring Design and Analysis
... The reference **post** is on the south side of the road ... 22, 27, 32, 37, 42, and 47 **meters** along the ... of the starting point for systematic sampling must be **random**. ...
fire.r9.fws.gov/ifcc/monitor/RefGuide/ study_design_and_analysis.htm - 46k - Cached - Similar pages

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

postage meter and random numb [Google Search] Search within results

Dissatisfied with your search results? Help us improve.

Get the Google Toolbar: Google - Search Web - PageRank 6 blocked Auto

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google

Google

Advanced Search Preferences Language Tools Search Tips

franking machine and cryptograp [Google Search]

The "AND" operator is unnecessary – we include all search terms by default. [details]

Web · Images · Groups · Directory · News ·

Searched the web for **franking machine and cryptographic keys**. Results **1** - **10** of about **13,800**. Search took 0

By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

[PDF] FPSM Security Policy Version 1.4
File Format: PDF/Adobe Acrobat - View as HTML
... register sets store the amount of money to be **franked** by the **franking machine**. ... **Keys**
(SRDI) KE This item stands for all of the **cryptographic keys** stored inside ...
csrc.nist.gov/cryptval/140-1/140sp/140sp062.pdf - Similar pages

Thales
... the traditional stamps or **franking machines** by using ... offices or associations, PC
franking offers its users ... range, manages the **cryptographic keys** and ensures ...
security.thalesgroup.com/case_study/case6.htm - 25k - Cached - Similar pages

[PPT] WPI Fall 2003 Semester EE579S/CS525 Computer Security
File Format: Microsoft Powerpoint 97 - View as HTML
... No place for **Frank** to get in the middle. ... A **machine** stores high-quality secret;
a person memorizes low-quality password. **Cryptographic** operations. ...
ece.wpi.edu/~wjlou/htmls/teaching/NOTE-0930.ppt - Similar pages

World-Information.Org
... by WF Friedman or his colleague **Frank** Rowlett - at ... similar to the German Enigma **machine**
1943 Colossus ... Bletchley Park 1943-1980 the **cryptographic** Venona Project ...
www.world-information.org/wio/infostructure/ 100437611776/100438658921?opmode=contents - 41k - Cached - Similar pages

Brute force attacks on **cryptographic keys**
... **Frank** Hoornaert, Jo Goubert, and Yvo Desmedt ... A **machine** to break **keys** at one per day would ... **Cryptographic** Hardware and Embedded Systems, LNCS 1717, Springer-Verlag ...
www.cl.cam.ac.uk/~rnc1/brute.html - 26k - Cached - Similar pages

[PDF] WebSentry™ Secures the First Live Electronic Stamping System
File Format: PDF/Adobe Acrobat - View as HTML
... **Franking Machines** and Printed Stamps... A Thing of the ... of the new Public **Key** Infrastructure (PKI ... WebSentry™ Ethernet offers **Cryptographic** Acceleration, High ...
www.thales-esecurity.com/CaseStudies/ Documents/Stampit_Case_Study.pdf - Similar pages

Thales e-Security solutions for electronic payments and ...
... STAMPIT service complements the traditional **franking machines** by using ... to simplify the letter **franking** process ... range, manages the **cryptographic keys** and ensures ...
www.thales-esecurity.com/Newsroom/ Releases2003/20020627.shtml - 26k - Cached - Similar pages

IT Management: Enterprise Applications
... in Software Security By Brad Arkin **Frank** Hill Scott ... to invent special **machines** to crack **cryptographic** algorithms ... EFF created a special-purpose **machine** to crack ...
itmanagement.earthweb.com/entdev/ print.php/11070_616221_3 - 21k - Cached - Similar pages

SINTRA - Distributing Trust on the Internet
... The service uses state-**machine** replication and ... Christian Cachin, Klaus Kursawe, **Frank** Petzold, and ... These **cryptographic** protocols have practical and provably ...
www.zurich.ibm.com/security/dti/ - 16k - Cached - Similar pages

ATIP95.42 : **Cryptography** & Smart Cards: Policy + Algorithms
... impossible to separate **cryptographic** technology from ... DTH) Automatic teller **machines** Electronic funds ... ticket terminals Postal **franking machines** Medical record ...
www.cs.arizona.edu/japan/www/atip/public/ atip.reports.95/atip95.42r.html - 33k - Cached - Similar pages

Goooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

franking machine and cryptograp | Google Search | Search within results

Dissatisfied with your search results? Help us improve.

Get the Google Toolbar:

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

Google

Advanced Search Preferences Language Tools Search Tips

postage metering and cryptograp Google Search

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web · Images · Groups · Directory · News ·

Searched the web for **postage metering and cryptographic keys**. Results **1** - **10** of about **1,840**. Search took **0.**

By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

SPYRUS Press -- SPYRUS Unveils Electronic **Postage Metering**
... order to guarantee **postage** integrity, accurate ... fraud, SPYRUS' public **k y cryptographic**
technologies are ... certificate processing and electronic money **metering**. ...
www.spyrus.com.au/content/pressroom/ releases/1998/pr_neopost.asp - 21k - Cached - Similar pages

[PDF] Electronic **Postage**
File Format: PDF/Adobe Acrobat - View as HTML
... electronic **postage metering** devices and for online PC ... of CCD cameras, high speed **cryptographic**
equipment for ... making the transition towards electronic **postage**. ...
www.win.tue.nl/~henkvt/GBI.E-Postage.pdf - Similar pages

[PDF] **Cryptographic** Module Validation Program **Cryptographic** Module ...
File Format: PDF/Adobe Acrobat - View as HTML
... Policy, Finite State Model, **Key** Management Document ... configuration – eg software
applications, **cryptographic** toolkits, **postage metering** devices, radio ...
www.rsaconference.com/rsa2003/europe/tracks/
pdfs/developers_w15_tencati.pdf - Similar pages

Designing **Cryptographic Postage** Indicia - Heintze, Tygar, Yee ...
... this idea to develop a secure **postal metering** system for ... JD Tygar, and B. Yee, Designing
cryptographic postage indicia, In ... digital signatures and public-**key** cry ...
citeseer.nj.nec.com/heintze96designing.html - 24k - Cached - Similar pages

Cryptographic Postage Indicia - Heintze, Tygar, Yee (ResearchIndex ...
... types of improper use of **metering** indicia. ... the sentence level): 73.2%: Designing **Cryptographic**
Postage Indicia - TYGAR ... **Cryptographic Postage** Indicia." To appear ...
citeseer.nj.nec.com/184431.html - 25k - Cached - Similar pages
[More results from citeseer.nj.nec.com]

SDG Services
... of applications using public **key** infrastructure components ... 1 compliant

software **crypt graphic**
module for ... States **Postal** Service **p stage metering** standards as ...
www.corsec.com/soft_sdg.php - 8k - Cached - Similar pages

[PDF] Distributed Computing: Introduction Distributed Computing ...
File Format: PDF/Adobe Acrobat - View as HTML
... coprocessor – Securely maintains **postage** balance – Cryptographical y ... to read off **cryptographic key** • Typical MOS ... Will become dominant form of **metering**
www.sims.berkeley.edu/courses/is206/ f99/slides_revised/8-26.pdf - Similar pages

Publications: Internet **Postage** - Becker & Poliakoff
... file transfer protocol, public **key** infrastructure, **cryptographic** ... that performs the **cryptographic** (coding and ... Previously, **postage metering** systems only had to ...
www.becker-poliakoff.com/publications/ article_archive/internet_postage.htm - 22k - Cached - Similar pages

Computergram International: CYLINK SIGNS OFF ON US **POSTAL** ...
... medium-sized businesses, to download **postage** value to ... designed to replace the current **metering** system used ... Public-**key cryptography**, which was invented in 1976 ...
www.findarticles.com/cf_dls/m0CGN/ n161/21020905/p1/article.jhtml - 15k - Cached - Similar pages

[PDF] EVENECTOR
File Format: PDF/Adobe Acrobat - View as HTML
... deployed in thousands of electronic **postage metering** devices of ... generator for its electronic **postage** meters ... bit data, 2 bit addresses **Cryptographic** Gear Ciphers ...
www.revenector.com/Revenector_Full.pdf - Similar pages

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

postage metering and cryptograp [Google Search] Search within results

Dissatisfied with your search results? Help us improve.

Get the Google Toolbar: Google ▾ [▾] Search Web ▾ PageRank 6 blocked Aut

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google

Google

Advanced Search Preferences Language Tools Search Tips

postage metering and cryptograp Google Search

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web · Images · Groups · Directory · News ·

Searched the web for **postage metering and cryptographic keys**. Results **21** - **30** of about **1,840**. Search took (

By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

Patent Database Search Results: isd/19760101->20000725 and (ccl ...
... 107. 4,809,186 **Postage** meter for **metering** mixed weight ... 4,771,461 Initialization
of **cryptographic** variables in an EFT/POS network with a large number of ...
www.ondapatent.com/Japanese/business/trans_3.html - 13k - Cached - Similar pages

Cryptographic Postage Indicia - Heintze, Tygar, Yee (ResearchIndex ...
... several types of improper use of **metering** indicia. ... obtaining digital signatures and
public-**key** cryptosystems; Communic ... **Cryptographic Postage** Indicia." To appear ...
citeseer.ist.psu.edu/184431.html - 25k - Cached - Similar pages

[PS] **Cryptographic Postage** Indicia JD Tygar Bennet S. Yee Nevin Heintze ...
File Format: Adobe PostScript - View as Text
... 19. JD Tygar, Bennet S. Yee, and Nevin Heintze. **Cryptographic postage**
indicia. ... **Metering** Devices, May 1995. 21. US **Postal** Service. ...
www.bennetyee.org/ucsd-pages/pub/asian-96.ps - Similar pages

List of Validated Products under **Cryptographic** Module Validation ...
... 256, N90i Secure **Metering** Moddule (SMM) (Hardware ... 202, TrustField TM **Cryptographic**
Key Server, CKS Model 2000 ... 201, PROmail II (Simply **Postage** III) (Hardware Version ...
www.cse-cst.gc.ca/en/services/industrial_services/ cmv_val_products.html - 101k - Cached - Similar pages
[More results from www.cse-cst.gc.ca]

DREI97 SPEAKER LIST
... **Key** Management in the **Post**-Identity Era ... Kevin McCurley, IBM - Research, "**Cryptographic**
Number Theory ... AT&T Labs - Research, "Auditable **Metering** with Lightweight ...
dimacs.rutgers.edu/drei/1997/schedule/Speaker-list.htm - 27k - Cached - Similar pages

Dallas Semiconductor turns on Internet commerce at the touch

of ...
... anticipated during the design of the **Cryptographic** iButton ... and audit trail for microcash
metering or other ... that it will replace its current **p stage** meters using ...
cypherpunks.venona.com/date/1996/10/msg00600.html - 10k - Cached - Similar pages

CFP: Applied **Cryptography** and Network Security
... modeling, light-weight **cryptography**, efficient protocols ... protection: protocols, implementations, **metering**, watermarking, digital ... at the **postal** address below. ...
www.cs.utah.edu/flux/cipher/cfps/cfp-ACNS04.html - 8k - Cached - Similar pages

Johann Bezuidenhoudt's Home Page
... An earlier version, entitled **Cryptographic** Credit Control in Pre-Payment **Metering** Systems, appeared at ... with a specific job of work (**post**) and the risk ...
users.iafrica.com/s/sj/sjb/ - 9k - Cached - Similar pages

[PDF] Hardware **Metering**
File Format: PDF/Adobe Acrobat - View as HTML
... Modern **cryptography** started with introduction of one-way ... For this reason, we suggest **post**-processing, ie ... 4. HARDWARE **METERING** TECHNIQUES In this section, we ...
www.cs.ucla.edu/~farinaz/papers/DAC30_4.pdf - Similar pages

POSTAL SERVICE
... with current regulations for **metering** products (CFR ... or transmission of software and **cryptographic keys**. ... The Manager, **Postage** Technology Management will provide ...
www.usps.com/postagesolutions/_doc/sub031.html - 101k - Cached - Similar pages

◀ Goooooooooooogle ▶
Result Page: **Previous** 1 2 3 4 5 6 7 8 9 10 11 12 **Next**

postage metering and cryptograp | Google Search | Search within results

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google

Advanced Search Preferences Language Tools Search Tips

postage metering and cryptograp [Google Search]

The "AND" operator is unnecessary – we include all search terms by default. [details]

Web · Images · Groups · Directory · News ·

Searched the web for **postage metering and cryptographic keys**. Results **41** - **50** of about **1,840**. Search took (

By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

Free Public **Key** Infrastructure White Papers, Webcasts and Product ...
... applicable to any application employing **cryptography**. ... Internet Security | Public **Key**
Infrastructure, by ... infrastructure security and **metering** software, provides ...
techlibrary.wallstreetandtech.com/ data/rlist?t=987097377_11107759 - 54k - Cached - Similar pages

[PDF] A Survey of **Cryptography** Algorithms – Trends and Products
File Format: PDF/Adobe Acrobat - View as HTML
... Hellman [9] in 1976 and published in the ground-breaking paper "New Directions in
Cryptography." The protocol allows two users to exchange a secret **key** over an ...
www.netmode.ntua.gr/courses/postgraduate/edi/assign/ 2000/Cryptography_algorithms_report.pdf - Similar pages

CommWeb: Public **Key** Infrastructure
... significance of sound **key** management applicable to any application employing **cryptography**. ... infrastructure
security and **metering** software, provides ...
techlibrary.commweb.com/data/ rlist?t=987097377_11107759 - 56k - Cached - Similar pages

[PDF] **Cryptographic** Products IBM PCI **Cryptographic** Coprocessor General ...
File Format: PDF/Adobe Acrobat - View as HTML
... of these very | sensitive and hard-to-replace **keys**. ... via the the IBM Common **Cryptographic**
Architecture API ... For example, **postage metering** applications run in an ...
www.cs.dartmouth.edu/~jerryw/thesis/4758_Gen_Info.pdf - Similar pages

[PPT] Digital Rights Management Business and Technology
File Format: Microsoft Powerpoint 97 - View as HTML
... 2002. Usage **Metering**. Legacy online services. ... 2002. **Cryptography** and DRM.
Encrypting content. ... Like barcodes on products. Microdots used by US **Postal** Service. ...
www.giantstepsmts.com/old/msftvit/ Digital%20Rights%20Management% 20overview.ppt - Similar pages

authentication Innovations and Patents

... secure processing of **postal** data 6,381,454 ... financial messaging unit 6,378,072: **Cryptographic** system 6,378,071 ... for processing communication **metering** data 6,377,809 ...
www.prime-radiant.com/technologies/authentication.html - 53k - Cached - Similar pages

[PDF] Economics of **Postage** Payment and Mailer-**Post** Interface
File Format: PDF/Adobe Acrobat - View as HTML
... However, due to several limitations the **metering** system was ... through the use of a **cryptographic key** shared or ... use of a franking system or "**postage** meter" to ...
www.postinsight.pb.com/go.cfm?file=econpp.pdf - Similar pages

Security
... Seals; electronic **postal** indicia. Telecommunications security Attacks on **metering**, signalling, switching and configuration. ... Asymmetric **cryptographic** protocols. ...
www.cl.cam.ac.uk/DeptInfo/CST/node66.html - 11k - Cached - Similar pages

EasyLicenser 2.0 from Agilis is released
... Public **key cryptography** is also combined with access-controlled ... accelerating the development process for ISVs using **metering**. ... in to be able to **post** a comment ...
www.programmersheaven.com/d/click.aspx?ID=N3068 - 23k - Cached - Similar pages

International Patent Applications (PCT Applications) for which ...
... 98-08325: Printing **postage** with **cryptographic** clocking security; 98 ... 97-40602: Secure smart card access to pre-paid **metering** funds in a computer; 97-40600 ...
www.patents.com/oandl/pcts.htm - 17k - Cached - Similar pages

◀ Goooooooooooooogle ▶

Result Page: **Previous** 1 2 3 4 **5** 6 7 8 9 10 11 12 13 14 **Next**

postage metering and cryptograp | Google Search | Search within results

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google

PORTAL
THE ACM DIGITAL LI RARY

> home > about > feedback > login
US Patent & Trademark Office

Try the *new* Portal design
Give us your opinion after using it.

Search Results

Search Results for: **[random number and cryptographic keys]**
Found **45** of **124,998 searched.**

Search within Results

> Advanced Search
> Search Help/Tips

S rt by: Title Publication Publication Date Score Binder

Results 1 - 20 of 45 short listing

Prev Page 1 2 3 Next Page

1 Crypto backup and key escrow 85%
David Paul Maher
Communications of the ACM March 1996
Volume 39 Issue 3

2 The KryptoKnight family of light-weight protocols for authentication and key distribution 84%
Ray Bird , Inder Gopal , Amir Herzberg , Phil Janson , Shay Kutten , Refik Molva , Moti Yung
IEEE/ACM Transactions on Networking (TON) February 1995
Volume 3 Issue 1

3 Security & transport: Mobility helps security in ad hoc networks 80%
Srdjan Capkun , Jean-Pierre Hubaux , Levente Buttyán
Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing June 2003

> Contrary to the common belief that mobility makes security more difficult to achieve, we show that node mobility can, in fact, be useful to provide security in ad hoc networks. We propose a technique in which security associations between nodes are established, when they are in the vicinity of each other, by exchanging appropriate cryptographic material. We show that this technique is generic, by explaining its application to fully self-organized ad hoc networks and to ad hoc networks placed und ...

4 Optimal algorithms for Byzantine agreement 80%
Paul Feldman , Silvio Micali
Pr ceedings f the twentieth annual ACM symp sium n The ry f c mputing

January 1988

We exhibit randomized Byzantine agreement (BA) algorithms achieving optimal running time and fault tolerance against all types of adversaries ever considered in the literature. Our BA algorithms do not require trusted parties, preprocessing, or non-constructive arguments. Given private communication lines, we show that n processors can reach BA in expected constant time in a syncronous network if any <

5 Muscle Flexes Smart Cards into Linux 80%

David Corcoran

Linux Journal August 1998

The newest kind of card for your pocketbook offers better security for the information it holds

6 Efficient coloring of a large spectrum of graphs 80%

Darko Kirovski , Miodrag Potkonjak

Proceedings of the 35th annual conference on Design automation conference May 1998

We have developed a new algorithm and software for graph coloring by systematically combining several algorithm and software development ideas that had crucial impact on the algorithm's performance. The algorithm explores the divide-and-conquer paradigm, global search for constrained independent sets using a computationally inexpensive objective function, assignment of most-constrained vertices to least-constraining colors, reuse and locality exploration of intermediate solutions, s ...

7 Secure communication using remote procedure calls 80%

Andrew D. Birrell

ACM Transactions on Computer Systems (TOCS) February 1985

Volume 3 Issue 1

Research on encryption-based secure communication protocols has reached a stage where it is feasible to construct end-to-end secure protocols. The design of such a protocol, built as part of a remote procedure call package, is described. The security abstraction presented to users of the package, the authentication mechanisms, and the protocol for encrypting and verifying remote calls are also described.

8 A survey of key management for secure group communication 77%

Sandro Rafaeli , David Hutchison

ACM Computing Surveys (CSUR) September 2003

Volume 35 Issue 3

Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing nongroup members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members, distributing the cryptographic keys becomes an issue. Researchers have proposed several different approach ...

9 Intrusion detection: Countering code-injection attacks with instruction-set randomization 77%

Gaurav S. Kc , Angelos D. Keromytis , Vassilis Prevelakis

Pr ceedings f the 10th ACM c nference n C mputer and c mmunicati n security October 2003

We describe a new, general approach for safeguarding systems against *any* type of code-injection attack. We apply Kerckhoff's principle, by creating process-specific randomized instruction sets (*e.g.,* machine instructions) of the system executing potentially vulnerable software. An attacker who does not know the key to the randomization algorithm will inject code that is invalid for that randomized processor, causing a runtime exception. To determine the difficulty of integrating su ...

10 Power modeling and optimization for embedded systems: Energy-efficient data scrambling on memory-processor interfaces 77%

Luca Benini , Angelo Galati , Alberto Macii , Enrico Macii , Massimo Poncino
Proceedings of the 2003 international symposium on Low power electronics and design August 2003

Crypto-processors are prone to security attacks based on the observation of their power consumption profile. We propose new techniques for increasing the non-determinism of such profile, which rely on the idea of introducing randomness in the bus data transfers. This is achieved by combining data scrambling with energy-efficient bus encoding, thus providing high information protection at no energy cost.Results on a set of bus traces originated by real-life applications demonstrate the applicabil ...

11 Some cryptographic principles of authentication in electronic funds transfer systems 77%

C. H. Meyer , S. M. Matyas
Proceedings of the seventh symposium on Data communications October 1981

One essential requirement of an Electronic Funds Transfer (EFT) system is that institutions must be able to join together in a common EFT network such that a member of one institution can initiate transactions at entry points in the domain of another institution. The use of such a network is defined as interchange. Cryptographic implementations are developed for such a network in such a way as to keep personal verification and message authentication processes at diffe ...

12 Chord: a scalable peer-to-peer lookup protocol for internet applications 77%

Ion Stoica , Robert Morris , David Liben-Nowell , David R. Karger , M. Frans Kaashoek , Frank Dabek , Hari Balakrishnan
IEEE/ACM Transactions on Networking (TON) February 2003
Volume 11 Issue 1

A fundamental problem that confronts peer-to-peer applications is the efficient location of the node that stores a desired data item. This paper presents *Chord*, a distributed lookup protocol that addresses this problem. Chord provides support for just one operation: given a key, it maps the key onto a node. Data location can be easily implemented on top of Chord by associating a key with each data item, and storing the key/data pair at the node to which the key maps. Chord adapts efficien ...

13 Anonymous E-prescriptions 77%

Giuseppe Ateniese , Breno de Medeiros
Proceeding of the ACM workshop on Privacy in the Electronic Society November 2002

This paper studies issues related to privacy protection of medical data, arguing that the topic is suitable for applied cryptographic research.We present the problem of medicine prescription privacy and describe a practical system that employs standard cryptographic techniques to achieve several improvements over current practices. We also introduce a very simple tool: Online group signatures which can be built via simple primitives implemented in commonly employed cryptographic libraries.

14 SPINS: security protocols for sensor networks 77%

Adrian Perrig , Robert Szewczyk , J. D. Tygar , Victor Wen , David E. Culler

Wireless Netw rks September 2002

Volume 8 Issue 5

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

15 Key management and key exchange: A key-management scheme for distributed sensor networks 77%

Laurent Eschenauer , Virgil D. Gligor

Proceedings of the 9th ACM conference on Computer and communications security November 2002

Distributed Sensor Networks (DSNs) are ad-hoc mobile networks that include sensor nodes with limited computation and communication capabilities. DSNs are dynamic in the sense that they allow addition and deletion of sensor nodes after deployment to grow the network or replace failing and unreliable nodes. DSNs may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary. Hence DSNs require cryptographic protection of com ...

16 Security and Middleware Services: Efficient and secure keys management for wireless mobile communications 77%

Roberto Di Pietro , Luigi V. Mancini , Sushil Jajodia

Proceedings of the second ACM international workshop on Principles of mobile computing October 2002

This paper presents an efficient algorithm for the secure group key management of mobile users. The most promising protocols to deal with group key management are those based on logical key hierarchy (LKH). The LKH model reduces to logarithmic size the resources needed: computation time, message exchanged, and memory space. In the framework of the LKH model, we present a new protocol LKH++ that outperforms the other proposed solutions in the literature. Such performance improvements are obtained ...

17 Token-based scanning of source code for security problems 77%

John Viega , J. T. Bloch , Tadayoshi Kohno , Gary McGraw

ACM Transactions on Information and System Security (TISSEC) August 2002

Volume 5 Issue 3

We describe **ITS4**, a tool for statically scanning C and C++ source code for security vulnerabilities. Compared to other approaches, our scanning technique stakes out a new middle ground between accuracy and efficiency. This method is efficient enough to offer real-time feedback to developers during coding while producing few false negatives. Unlike other techniques, our method is also simple enough to scan C++ code despite the complexities inherent in the language. Using **ITS4**, we fo ...

18 Session 1: Applications: New directions for integrated circuit cards operating systems 77%

Pierre Paradinas , Jean-Jacques Vandewalle

Pr ceedings f the 6th w rksh p n ACM SIGOPS European w rksh p: Matching

perating systems t applicati n needs September 1994

Integrated circuit cards or smart cards are now well-known. Applications such as electronic purses (cash units stored in cards), subscriber identification cards used in cellular telephone or access keys for pay-TV and information highways emerge in many places with millions of users. More services are required by applications providers and card holders. Mainly, new integrated circuit cards evolve towards non-predefined multi-purpose, open and multi-user applications. Today, operating systems imp ...

19 Mobile Code and Distributed Systems: A new approach to DNS security (DNSSEC) 77%

Giuseppe Ateniese , Stefan Mangard

Proceedings of the 8th ACM conference on Computer and Communications Security November 2001

The Domain Name System (DNS) is a distributed database that allows convenient storing and retrieving of resource records. DNS has been extended to provide security services (DNSSEC) mainly through public-key cryptography. We propose a new approach to DNSSEC that may result in a significantly more efficient protocol. We introduce a new strategy to build chains of trust from root servers to authoritative servers. The techniques we employ are based on symmetric-key cryptography.

20 Secure password-based cipher suite for TLS 77%

ACM Transactions on Information and System Security (TISSEC) May 2001 Volume 4 Issue 2

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Results 1 - 20 of 45 **short listing**

Prev Page 1 2 3 Next Page

> home > about > feedback > login

US Patent & Trademark Office

Try the *new* Portal design

Give us your opinion after using it.

Search Results

Search Results for: **[random number and cryptographic keys]**
Found **45** of **124,998 searched.**

Search within Results

> Advanced Search

> Search Help/Tips

S rt by: Title Publication Publication Date Score Binder

Results 21 - 40 of 45 **short listing**

Prev Page 1 2 3 Next Page

21 SPINS: security protocols for sensor netowrks 77%
Adrian Perrig , Robert Szewczyk , Victor Wen , David Culler , J. D. Tygar
Proceedings of the 7th annual international conference on Mobile computing and networking July 2001

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security.

We present a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and &mgr;TESLA SNEP provides the following important baseline security primitives: Data confidentia ...

22 Cryptographic solution to a problem of access control in a hierarchy 77%
Selim G. Akl , Peter D. Taylor
ACM Transactions on Computer Systems (TOCS) August 1983
Volume 1 Issue 3

23 Encryption and Secure Computer Networks 77%
Gerald J. Popek , Charles S. Kline
ACM Computing Surveys (CSUR) December 1979
Volume 11 Issue 4

24 Cryptographic sealing for information secrecy and authentication 77%
David K. Gifford
C mmunicati ns f the ACM April 1982

Volume 25 Issue 4

A new protection mechanism is described that provides general primitives for protection and authentication. The mechanism is based on the idea of sealing an object with a key. Sealed objects are self-authenticating, and in the absence of an appropriate set of keys, only provide information about the size of their contents. New keys can be freely created at any time, and keys can also be derived from existing keys with operators that include Key-And and Key-Or

25 Advanced cryptographic techniques for computer 77%

Dennie Van Tassel

Communications of the ACM December 1969

Volume 12 Issue 12

Cryptographic techniques which can be used to maintain the confidentiality of information processed by computers are dealt with. Special emphasis is paid to the unique characteristics of computer files that make many cryptographic methods of little use. Relative security, costs, and preferred methods are included in this paper.

26 Towards a secure platform for distributed mobile object computing 77%

Marc Lacoste

ACM SIGOPS Operating Systems Review April 2000

Volume 34 Issue 2

We present some issues relevant to the design of a secure platform for distributed mobile computing, that goes beyond existing ad-hoc approaches to software mobility. This platform aims to support wide-area computing applications such as active network infrastructures or network supervision tools. Our contribution is two-fold: the first part of the paper is a survey of the security features of a few languages and virtual machines as regards authentication, access control, and communications secu ...

27 Specification, validation, and synthesis of email agent controllers: A case study in function rich reactive system design 77%

Robert J. Hall

Proceedings of the third workshop on Formal methods in software practice August 2000

With a few exceptions, previous formal methods for reactive system design have focused on finite state machines represented in terms of boolean states and boolean next-state functions. By contrast, in many reactive system domains requirements engineers and developers think in terms of complex data types and expressive next-state functions. Formal methods for reactive system design must be extended to meet their needs as well. I term a reactive system function rich if expr ...

28 Unlinkable serial transactions: protocols and applications 77%

Stuart G. Stubblebine , Paul F. Syverson , David M. Goldschlag

ACM Transactions on Information and System Security (TISSEC) November 1999

Volume 2 Issue 4

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

77%

29 Using smartcards to secure a personalized gambling device
William A. Aiello , Aviel D. Rubin , Martin J. Strauss
Pr ceedings f the 6th ACM c nference n C mputer and c mmunicati ns security November 1999

We introduce a technique for using an untrusted device, such as a hand-held personal digital assistant or a laptop to perform real financial transactions without a network. We utilize the tamper-resistant nature of smartcards to store value on them and perform probabilistic computations based on user input. We discuss an application of this to gambling. The technique has the properties that the user is guaranteed to make money when he wins and the house is guaranteed to make money w ...

30 The proactive security toolkit and applications 77%
Boaz Barak , Amir Herzberg , Dalit Naor , Eldad Shai
Proceedings of the 6th ACM conference on Computer and communications security November 1999

Existing security mechanisms focus on prevention of penetrations, detection of a penetration and (manual) recovery tools Indeed attackers focus their penetration efforts on breaking into critical modules, and on avoiding detection of the attack. As a result, security tools and procedures may cause the attackers to lose control over a specific module (computer, account), since the attacker would rather lose control than risk detection of the attack. While controlling the module, attacker may ...

31 A public-key based secure mobile IP 77%
John Zao , Joshua Gahm , Gregory Troxel , Matthew Condell , Pam Helinek , Nina Yuan , Isidro Castineyra , Stephen Kent
Wireless Networks October 1999
Volume 5 Issue 5

32 Smart Cards and Biometrics: The cool way to make secure transactions 77%
David Corcoran , David Sims , Bob Hillhouse
Linux Journal March 1999

33 Server-assisted cryptography 77%
Donald Beaver
Proceedings of the 1998 workshop on New security paradigms January 1998

34 Simplified VSS and fast-track multiparty computations with applications to threshold cryptography 77%
Rosario Gennaro , Michael O. Rabin , Tal Rabin
Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing June 1998

35 Proactive public key and signature systems 77%
Amir Herzberg , Markus Jakobsson , Stanislław Jarecki , Hugo Krawczyk , Moti Yung
Proceedings of the 4th ACM conference on Computer and communications security April 1997

36 Verifiable partial key escrow 77%
Mihir Bellare , Shafi Goldwasser
Pr ceedings of the 4th ACM c nference n C mputer and communicati ns

security April 1997

37 A calculus for cryptographic protocols: the spi calculus 77%
Martín Abadi , Andrew D. Gordon
Pr ceedings f the 4th ACM c nference n C mputer and c mmunicati ns security April 1997

38 A public-key based secure mobile IP 77%
John Zao , Stephen Kent , Joshua Gahm , Gregory Troxel , Matthew Condell , Pam Helinek , Nina Yuan , Isidro Castineyra
Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking September 1997

39 Maintaining authenticated communication in the presence of break-ins 77%
Ran Canetti , Shai Halevi , Amir Herzberg
Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing August 1997

40 Securing ATM networks 77%
Shaw-Cheng Chuang
Proceedings of the 3rd ACM conference on Computer and communications security January 1996

Results 21 - 40 of 45 **short listing**
Prev Page 1 2 3 Next Page

PORTAL
THE ACM DIGITAL LIBRARY

> home : > about : > feedback : > login

US Patent & Trademark Office

Try the *new* Portal design

Give us your opinion after using it.

Search Results

Search Results for: **[random number and cryptographic keys]**
Found **45** of **124,998 searched.**

Search within Results

> Advanced Search

> Search Help/Tips

S rt by: Title Publication Publication Date Score Binder

Results 41 - 45 of 45 **short listing**

Prev Page 1 2 3 Next Page

41 Securing the internet protocol 77%
Pau-Chen Cheng , Juan A. Garay , Amir Herzberg , Hugo Krawczyk
Proceedings of the fourteenth annual ACM symposium on Principles of distributed computing August 1995

42 New directions for integrated circuit cards operating systems 77%
Pierre Paradinas , Jean-Jacques Vandewalle
ACM SIGOPS Operating Systems Review January 1995
Volume 29 Issue 1

Integrated circuit cards or smart cards are now well-known. Applications such as electronic purses (cash units stored in cards), subscriber identification cards used in cellular telephone or access keys for pay-TV and information highways emerge in many places with millions of users. More services are required by applications providers and card holders. Mainly, new integrated circuit cards evolve towards non-predefined multi-purpose, open and multi-user applications. Today, operating systems imp ...

43 Authentication in the Taos operating system 77%
Edward Wobber , Martín Abadi , Michael Burrows , Butler Lampson
ACM Transactions on Computer Systems (TOCS) February 1994
Volume 12 Issue 1

We describe a design for security in a distributed system and its implementation. In our design, applications gain access to security services through a narrow interface. This interface provides a notion of identity that includes simple principals, groups, roles, and delegations. A new operating system component manages principals, credentials, and secure channels. It checks credentials according to the formal rules of a logic of authentication. Our implementation is efficient enough to sup ...

44 Extending cryptographic logics of belief to key agreement protocols 77%

Paul van Oorschot

Pr ceedings f the 1st ACM c nference n Computer and c mmunicati ns security December 1993

The authentication logic of Burrows, Abadi and Needham (BAN) provided an important step towards rigourous analysis of authentication protocols, and has motivated several subsequent refinements. We propose extensions to BAN-like logics which facilitate, for the first time, examination of public-key based authenticated key establishment protocols in which both parties contribute to the derived key (i.e. key agreement protocols). Attention is focussed on six distinct generic goals for authenti ...

45 Conditionally secure secret sharing schemes with disenrollment capability 77%

Chris Charnes , Josef Pieprzyk , Rei Safavi-Naini

Proceedings of the 2nd ACM Conference on Computer and communications security November 1994

The paper describes an implementation of Shamir secret sharing schemes based on exponentiation in Galois fields. It is shown how to generate shares so the scheme has the disenrollment capability. Next a family of conditionally secure Shamir schemes is defined and the disenrollment capability is investigated for the family. The paper also examines a problem of covert channels which are present in any secret sharing scheme.

Results 41 - 45 of 45 **short listing**

Prev Page 1 2 3 Next Page